

ALB:MRM
F.# 2017R00542

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF AN APPLICATION
FOR A SEARCH WARRANT FOR:

INFORMATION ASSOCIATED WITH
DJC4774@YAHOO.COM THAT IS
STORED AT PREMISES CONTROLLED
BY YAHOO! INC.

TO BE FILED UNDER SEAL

**APPLICATION FOR A
SEARCH WARRANT FOR
INFORMATION IN
POSSESSION OF A PROVIDER**

17 31 289
Case No. 1

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, AARON SPIVACK, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for the contents of and information pertaining to DJC4774@YAHOO.COM ("SUBJECT ACCOUNT"), that is stored at premises controlled by YAHOO! INC. ("Yahoo!"), an electronic service and email provider headquartered at 701 First Avenue, Sunnyvale, California, 94089 from the time period of January 1, 2014 to the present. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Yahoo! to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B,

government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation. I have been a Special Agent of the FBI since October 2008, and am currently assigned to the New York Office. Since May 2010, I have been assigned to a Crimes Against Children squad. I have been assigned to investigate violations of criminal law relating to the sexual exploitation of children. I have gained expertise in this area through training in classes and daily work related to conducting these types of investigations. As part of my responsibilities, I have been involved in the investigation of numerous child pornography cases and have reviewed thousands of photographs depicting children (less than eighteen years of age) being sexually exploited by adults. Through my experience in these investigations, I have become familiar with methods of determining whether a child is a minor. I am also a member of the Eastern District of New York Project Safe Childhood Task Force.

3. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from my own personal participation in the investigation, my review of documents, my training and experience, and discussions I have had with other law enforcement personnel concerning the creation, distribution, and proliferation of child pornography. The FBI is investigating the production, possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2251, 2252 and 2252A.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 2252(a) have been committed by the user of the SUBJECT ACCOUNT. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband or fruits of this crime, as further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

7. In September, 2016, Yahoo! reported to the National Center For Missing and Exploited Children (NCMEC) that between September 11th and September 12th, 2016, the Yahoo! screen/user name “TZJY5BXBC4JWTRCTSIM3B4MVLE” uploaded 23 image files depicting child pornography over Yahoo! Messenger.¹ Yahoo provided that the above listed

¹ In my training and experience, I have learned that Yahoo! Inc. provides an on-line service called Yahoo! Messenger to the general public. Yahoo! Messenger is an instant messaging client provided by Yahoo. Instant Messaging (“IM”) is a form of real-time direct text-based communication between two or more people using shared clients. The text is conveyed via devices connected over a network such as the Internet. In addition to text, Yahoo’s software allows users with the most current updated versions to utilize its webcam service. This option enables users from distances all over the world to view others who have installed a webcam on their end.

screen/user name used Internet Protocol (IP) address 24.42.122.22 to upload 22 of the child pornography images and IP address 107.77.223.214² to upload one of the child pornography images. A description of three of the images is provided below. NCMEC created CyberTipline Report 14186669.

8. In October 2016, NCMEC reported the aforementioned information, previously provided by Yahoo!, to the New York Police Department's Internet Crimes Against Children Task Force (the NYPD). The NYPD served a subpoena to Time Warner Cable for subscriber information on IP address 24.42.122.22 for the time it was used to upload the child pornography files. Time Warner Cable provided that the IP address was assigned to David Cerqueira at the 9725 Allendale Street, Jamaica, New York, 11435 (the Jamaica Address) and was associated with phone number (718) 657-6612.

9. In response to a subpoena for information on the screen/user name, Yahoo! provided that the plain language user name for the screen/user name was "djc4774" (the SUBJECT ACCOUNT) and that the name associated with the SUBJECT ACCOUNT was "David Cerq." Yahoo! also provided that email addresses davidcerqueira@earthlink.net and

In order to obtain a Yahoo! Messenger account, a Yahoo! email account is required. The Yahoo! email user must download the Yahoo! Messenger program and sign in with the same credentials used for his/her Yahoo! email account. Therefore, the user is issued the same Yahoo ID for the messenger program and the email account.

² Using publically available databases I know that IP address 107.77.223.214 is owned by AT&T wireless. Based on my training and experience I know that AT&T wireless does not maintain subscriber information associated with IP addresses since AT&T using "natting" IP protocol, which means multiple users can be assigned the same IP address at the same time.

david@bestelectromech.com; phone numbers (347) 728-8598 and (718) 657-6612³; and the address 97-25 Allendale St, Jamaica, New York, 11435 (the Jamaica Address) are associated with the SUBJECT ACCOUNT.

10. The last four digits of the social security number for David Cerqueira are 4774. The FBI assesses that the SUBJECT ACCOUNT is derived from Cerqueira's initials (djc) and the last four numbers of his social security number (4774).

11. The following are descriptions of three of the child pornography images associated with the SUBJECT ACCOUNT and uploaded to Yahoo! Messenger between September 11th and September 12th, 2016:

- a. "Img.25-1.jpg" – This image depicts a fully nude female, approximately two or three years of age. The child is laying on a bed with her hands tied to the bed rail above her head and her feet tied, forcing her legs to be spread apart and exposing her genitals.
- b. "Img.24-1.jpg" – This image depicts a fully nude adult female holding a fully nude infant or toddler. The adult woman is spreading the buttocks of the child and is licking the anus/genital region of the child.
- c. "Img.19-1" – This image depicts a fully nude female, approximately one or two years of age laying on the ground with her legs in the air exposing her

³ As set forth above, the phone number (718) 657-6612 is associated with the Time Warner subscriber information for IP address 24.42.122.22 when it was used to upload the child pornography files identified above.

genitals. What appears to be an adult hand is visible with the finger penetrating the anus of the child.

- d. The remaining 20 files from the upload to Yahoo! Messenger between September 11th and September 12th, 2016, were also child pornography.

12. On March 13, 2017, the Honorable Lois Bloom, United States Magistrate Judge, issued a warrant authorizing a search of the Jamaica Address. On March 16, 2017, law enforcement agents executed the search warrant at the Jamaica Address.

13. David J. Cerqueira ("Cerqueira") was at the Jamaica Address at the time of the execution of the search warrant. Law enforcement agents participated in a voluntary interview of Cerqueira at that time. Cerqueira was advised of the identities of the interviewing agents and the nature of the interview. Cerqueira was advised that he was not under arrest and that he could discontinue the interview at any time.

14. In sum and substance, Cerqueira confirmed that he resides at the Jamaica Address. He further admitted that he had been receiving, distributing and viewing child pornography for approximately one year. He admitted to using the social media applications Kik and instant messenger applications such as Yahoo! Messenger, including the SUBJECT ACCOUNT, both to find and receive child pornography and to discuss the sexual exploitation of children. He also admitted to sending hundreds of image files depicting child pornography, including the three files described above. He further indicated that he had numerous images of child pornography on his cellular telephone.

15. As part of the search, law enforcement agents recovered, among other things, a cellular telephone. A preliminary review of the contents of the cellular telephone revealed

hundreds of video and picture files containing child pornography, including pictures showing infant and toddler bondage.

16. On March 16, 2017, Cerqueira was placed under arrest and charged with a violation of Title 18, United States Code, Section 2252(a)(2) (distribution of child pornography). Also on March 16, 2017, Cerqueira was arraigned before the Honorable Lois Bloom. Cerqueira was released on a \$250,000.00 bond.

17. Subsequent reviews of the cellular telephone recovered from Cerqueira, as well as reviews of other electronic devices of Cerqueira's which were recovered from the Jamaica Address have revealed hundreds of additional video and picture files with names that are indicative of child pornography and pictures showing infant and toddler bondage. Additionally, the reviews have revealed numerous stored chats, through various messaging services, that Cerqueira has engaged in with others regarding the exchange, distribution, receipt and possible production of child pornography. The review of Cerqueira's electronic devices also revealed the following: (1) that Cerqueira has been engaged in discussions regarding sexual contact with children and exchanging child pornography using Yahoo! Messenger since at least September of 2014 and (2) that Cerqueira has had been using Yahoo! Messenger since January of 2014.

18. Based upon information that Yahoo! provided to NCMEC, at or about the time at which Yahoo! detected the upload of child pornography, Yahoo! disabled the SUBJECT ACCOUNT.

19. On or about March 27, 2017, Yahoo! confirmed to the FBI that Yahoo! is still in possession of the contents of the SUBJECT ACCOUNT. On March 28, 2017, the FBI

submitted a request pursuant to Title 18, United States Code, Section 2703(f) to Yahoo! Inc.'s Legal Department/Subpoena Compliance requesting preservation of the contents of the SUBJECT ACCOUNT for a period of ninety days.

TECHNICAL INFORMATION REGARDING YAHOO!

Yahoo! E-mail

20. Based on my training and experience, and publicly available information, I have learned that Yahoo! Inc. provides a variety of on-line services, including e-mail access, to the general public. Yahoo! Inc. allows subscribers to obtain email accounts at the domain name yahoo.com, like the email account listed in Attachment A. Subscribers obtain a Yahoo! email account by registering with Yahoo! Inc. During the registration process, Yahoo! Inc. asks subscribers to provide basic personal information. Therefore, the computers of Yahoo! Inc. are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Yahoo! Inc. subscribers) and information concerning subscribers and their use of Yahoo! Inc. services, such as account access information, e-mail transaction information, and account application information.

21. In general, an e-mail that is sent to a Yahoo! Inc. subscriber is stored in the subscriber's "mail box" on Yahoo! Inc. servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Yahoo! Inc.'s servers indefinitely. The user can move and store messages in personal folders such as a "sent folder." In recent years, Yahoo! Inc., and other ISPs have provided their users with larger storage capabilities associated with the user's e-mail account. Yahoo! Inc., and other ISPs have allowed users to store up to one (1) terabyte of information associated with the account

on ISP servers. Based on conversations with other law enforcement officers with experience in executing and reviewing search warrants of e-mail accounts, I have learned that search warrants for e-mail accounts and computer systems have revealed stored e-mails sent and/or received many years prior to the date of the search.

22. When the subscriber sends an e-mail, it is initiated at the user's computer or mobile device, transferred via the Internet to Yahoo! Inc.'s servers, and then transmitted to its end destination. Yahoo! Inc. typically saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Yahoo! Inc. server, the e-mail can remain on the system indefinitely.

23. A sent or received e-mail typically includes the content of the message (including attachments), source and destination addresses, the date and time at which the e-mail was sent, and the size and length of the e-mail. If an e-mail user writes a draft message but does not send it, that message may also be saved by Yahoo! Inc. but may not include all of these categories of data.

24. A Yahoo! Inc. subscriber can also store files, including e-mails, address books, contact or buddy lists, calendar data, pictures, and other files, on servers maintained and/or owned by Yahoo! Inc. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

25. Many subscribers to Yahoo! Inc. do not store copies of the e-mails stored in their Yahoo! Inc. account on their home computers. This is particularly true because they access their Yahoo! Inc. account through the Internet, and thus it is not necessary to copy e-

mails to a home computer to use the service. Moreover, an individual may not wish to maintain particular e-mails or files in their residence to ensure others with access to the computer cannot access the e-mails.

26. In my training and experience, generally, e-mail providers like Yahoo! Inc. ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers (usually a mobile number) and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit card or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

27. The mobile number and alternate e-mail information provided to Yahoo! Inc., by the user are particularly useful in instances where a user needs to recover his/her account in the event of a lost password or account compromise. With these, Yahoo! Inc. can send a "reset password" link to the alternate e-mail address, or an SMS message to the mobile number. Upon receiving the "reset password" link to an SMS mobile number affiliated with that account, the user can then reset the password in order to continue to utilize that particular account. Because both a mobile device number and alternate e-mail address are used to recover access to an account, they both tend to be closely associated with the user of the account. It is important to note that though Yahoo! attempts to validate the personal

identifying information provided by subscribers, the validation requires additional voluntary input from users. As this additional input is voluntary, Yahoo! is not always successful in validating a user's personal identifying information.

28. When creating an account at Yahoo! Inc., the user is provided the opportunity to create a display name and an associated "Profile." Yahoo! Inc. allows a user to personalize their Profile by "adding an image that represents you." The display name and display image a user provides for their Profile is public and can be seen by anyone, even if the user chooses to keep the rest of their Profile hidden from other users.

29. In my training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Yahoo! Inc.'s website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

30. In my training and experience, in some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail

providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

31. In my training and experience, e-mail users often use e-mail accounts for everyday transactions because it is fast, low cost, and simple to use. People use e-mail to communicate with friends and family, manage accounts, pay bills, and conduct other online business. E-mail users often keep records of these transactions in their e-mail accounts, to include personal identifying information such as name and address.

32. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

33. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a

relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored in the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Lastly, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

Yahoo! Messenger

34. In my training and experience, I have also learned that Yahoo! Inc. provides an on-line service called Yahoo! Messenger to the general public. Yahoo! Messenger is an instant messaging client provided by Yahoo!. Instant Messaging ("IM") is a form of real-time direct text-based communication between two or more people using shared clients. The text is conveyed via devices connected over a network such as the Internet. In addition to text, Yahoo's software allows users with the most current updated versions to utilize its

webcam service. This option enables users from distances all over the world to view others who have installed a webcam on their end.

35. In order to obtain a Yahoo! Messenger account, a Yahoo! email account is required. The Yahoo! email user must download the Yahoo! Messenger program and sign in with the same credentials used for his/her Yahoo! email account. Therefore the user is issued the same Yahoo! ID for the messenger program and the email account.

36. The Terms of Service for a Yahoo! Messenger account state that a user's Yahoo! Messenger account is tied to that same user's Yahoo! email account. The Terms of Service also notify the user that Yahoo! Messenger will allow the user and the people the user communicates with to save those conversations and other information into the user's affiliated Yahoo! email account. Yahoo! Messenger also allows users to exchange computer to computer voice calls with their online contacts. If a user subscribes to the "Phone In" or "Phone Out" premium services, the user can also use Yahoo! Messenger to make or receive calls from regular telephones.

37. An individual must be a registered Yahoo! user in order to use Yahoo! Messenger. Yahoo! Messenger establishes a connection to the Internet when it is active -- much like a browser does -- in order for communications to be received and transmitted.

38. A user may archive Yahoo! instant messages along with Yahoo! email messages and search them together (in addition to Voice Mail, SMS, call history, and more). For users that have elected to archive their messages, Yahoo! Messenger will now archive messages on Yahoo! servers to establish and maintain this archive. Messages stored on Yahoo! servers in this manner are accessible from any computer system or device able to use


the latest versions of Yahoo! Messenger for computer. Users can view their Yahoo! Messenger conversation history and Yahoo! email archive (if they are tied to the same user ID) on Yahoo! Messenger through "Conversation History" in the settings. A user can turn off this feature for instant messages at any time by selecting "Do not keep a record of my conversations." Even if a user chooses not to save his message history, users with whom he communicates may opt to use the functionality available in their version of Yahoo! Messenger to save the communications and his conversations may be saved on Yahoo! servers, just like e-mail. Users can delete their archived messages by selecting the message, and clicking on the "Delete" button. However, this does not delete any of their conversations saved by other users. Yahoo! may analyze instant messages that users elect to archive in order to provide personally relevant product features, content, and advertising, and spam and malware detection.

39. In my training and experience, evidence of the true identity of the owner of an electronic account may be found in e-mail and/or instant messages, to include personal information, pictures, and residential or work place locations and addresses.

CONCLUSION

40. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Yahoo! who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



Aaron E. Spivack
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on March 30, 2017



Honorable Steven M. Gold
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with DJC4774@YAHOO.COM, a Yahoo! email and messenger account, that is stored at premises controlled by YAHOO! INC., a company that accepts service of legal process at 701 First Avenue, Sunnyvale, California, 94089, for the period of January 1, 2014 through the present.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by YAHOO! INC. (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on March 28, 2017, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, any attachments to such email, the date and time at which each email was sent, and the size and length of each email;
- b. The contents of all chats, Instant Messages (IM) and video chats associated with the account, including stored or preserved copies of chats and/or IMs sent to and from the account, the source and destination addresses associated with each of the chats and/or IMs, any attachments to the chats and/or IMs, the date and time at which each chat message and/or IM was sent and received, and the size and length of each chat and/or IM;
- c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods

of connecting, log files, and means and source of payment (including any credit or bank account number);

- d. The types of service utilized;
- e. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- f. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Section 2252, those violations involving DJC4774@YAHOO.COM and occurring after January 1, 2014, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Violations of Title 18, United States Code, Section 2252(a) (activities relating to material involving the sexual exploitation of minors);
- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (e) The identity of the person(s) who communicated with DJC4774@YAHOO.COM about matters relating to violations of Title 18, United States Code, Section 2252(a) (activities relating to material involving the sexual exploitation of minors), including records that help reveal their whereabouts.